Robert S. Green (State Bar No. 136183)
James Robert Noblin (State Bar No. 114442)
Evan M. Sumer (State Bar No. 329181)
GREEN & NOBLIN, P.C.
2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

Cornelius P. Dukelow, *admitted pro hac vice*
cdukelow@abingtonlaw.com
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)

William B. Federman, *admitted pro hac vice*
wbf@federmanlaw.com
Oklahoma Bar No. 2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

BRIGID POLING and DWIGHT JENKINS, individually and on behalf of all others similarly situated and on behalf of the general public, Plaintiff, v. ARTECH L.L.C., Defendant.	§	Case No. 3:20-cv-07630-LB **FIRST AMENDED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Brigid Poling ("Ms. Poling") and Dwight Jenkins ("Mr. Jenkins") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated and on behalf of the general public, allege the following against Defendant Artech L.L.C. ("Defendant" or "Artech") based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

BRIEF SUMMARY OF THE CASE

1. Defendant is a workforce solutions company providing managed services, contingent labor, staff augmentation, IT consulting, project outsourcing, and statement of work services across multiple industries, including systems integration, banking and finance, telecommunications, pharmaceutical & life sciences, energy, healthcare, technology, transportation, and local & federal government agencies.

2. On or about September 4, 2020, Defendant began notifying individuals, including Plaintiffs and other "Class Members" (Class Members is defined below) that on January 8, 2020, Defendant received a report of unusual activity relating to an employee's Artech user account. A subsequent investigation determined that an unauthorized actor gained access to certain of Defendant's computer systems between January 5, 2020 and January 8, 2020 (the "Data Breach").

3. Plaintiffs' and Class Members' data maintained on Defendant's computer systems and subject to the Data Breach included the types of sensitive personally identifiable information ("PII") that statutory and common law require companies to take security measures to protect: names, Social Security numbers, medical information, health insurance information, financial information, payment card information, driver's license/state identification numbers, government issued identification numbers, passport numbers, visa numbers, electronic/digital signatures, usernames and password information. This data should have received the most rigorous protection available – it did not.

4. Even though Defendant was storing sensitive PII that it knew was valuable to criminals, and vulnerable to exfiltration, Defendant failed to take security precautions necessary to protect Plaintiffs' and Class Members' data. Because Defendant failed to take necessary security precautions, Plaintiffs' and Class Members' unencrypted PII was accessed and acquired by an unauthorized person

or persons as a result of the Data Breach. As a result, Plaintiffs and Class Members have been harmed and face an increased risk of future harm.

PARTIES

5. Plaintiff Brigid Poling is an individual residing in Menlo Park, California. In mid- to late-September 2020, Plaintiff Poling received a "Notice of Data Breach" dated September 8, 2020, from Defendant (attached hereto as **Exhibit 1**) notifying her that her PII was compromised as a result of the Data Breach of Defendant's computer systems that took place between January 5, 2020, and January 8, 2020. The Notice of Data Breach specifically stated that Plaintiff Poling's name and Social Security number were accessed and acquired in the Data Breach. Plaintiff Poling's PII was in the possession, custody, and/or control of Defendant at the time of the Data Breach. Plaintiff Poling's PII remains in the possession, custody, and/or control of Defendant.

6. Since learning of the Data Breach, Plaintiff Poling has become worried that she will become a victim of identity theft or other fraud and has spent time investigating the Data Breach and attempting to mitigate potential future harm that may result from the Data Breach. Plaintiff Poling has also experienced an increase of spam texts and spam email and, as a direct and proximate result of the Data Breach, is now at a substantial and increased risk of future identity theft.

7. Plaintiff Dwight Jenkins is an individual residing in Wake Forest, North Carolina. In mid-to-late-September 2020, Plaintiff Jenkins received a Notice of Data Breach similar to the one received by Plaintiff Poling, which notified him that his PII was compromised as a result of the Data Breach. Plaintiff Jenkins has already fallen victim to identity theft as a result of the Data Breach, including unemployment accounts, bank accounts, and credit cards being opened in his name. Each of these instances of identity theft took place only weeks after the Data Breach. Plaintiff Jenkins' PII was in the possession, custody, and/or control of Defendant at the time of the Data Breach and remains in the possession, custody, and/or control of Defendant.

8. Since learning of the Data Breach, Plaintiff Jenkins has become a victim of identity theft and other fraud, is at a substantial and increased risk of additional identity theft in the future and has spent time investigating the Data Breach and attempting to mitigate current and potential future harm that may result from the Data Breach.

9. Defendant Artech L.L.C. is a New Jersey limited liability company with its principal place of business and global headquarters located in Morristown, New Jersey.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5,000,000 (exclusive of interests and costs), because there are more than 100 members in each of the proposed classes, and because at least one member of each of the proposed classes is a citizen of a State different from Defendant.

11. This Court has personal jurisdiction over Defendant because it regularly conducts business in California.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

STATEMENT OF FACTS

Defendant

13. Boasting more than 10,500 industry professionals in its employ, Defendant is a workforce solutions company maintaining operations in the US, Canada, India, and China. Defendant provides managed services, contingent labor, staff augmentation, IT consulting, project outsourcing, and statement of work services across multiple industries, including systems integration, banking and finance, telecommunications, pharmaceutical & life sciences, energy, healthcare, technology, transportation, and local & federal government agencies.

14. As part of its business operations, Defendant receives, collects, and maintains on its computer systems a large amount of sensitive PII which, when in the possession of unscrupulous individuals, may be used to commit various forms of fraud and identity theft.

The Data Breach

15. On or about September 4, 2020, Defendant began filing with various state Attorneys General a sample "Notice of Data Breach" letter (attached hereto as **Exhibit 2**), a "Notice of Data Event" statement (attached hereto as **Exhibit 3**), and a "Press Release" (attached hereto as **Exhibit 4**)

(collectively "Data Breach Notices") that mirrored the language of letters Defendant began mailing to Data Breach victims (including Plaintiff and Class Members) on or about that same date.

16. According to Defendant's "Data Breach Notices," Defendant discovered the Data Breach on January 8, 2020. The "Data Breach Notices" further state that "an unauthorized actor had access to certain Artech systems between January 5, 2020, and January 8, 2020."

17. According to the "Notice of Data Event" and "Press Release," Defendant's investigation determined that information accessed and acquired during the Data Breach potentially included the following: names, Social Security numbers, medical information, health insurance information, financial information, payment card information, driver's license/state identification numbers, government issued identification numbers, passport numbers, visa numbers, electronic/digital signatures, usernames and password information.

18. It is apparent from Defendant's "Data Breach Notices" that the PII accessed and acquired during the Data Breach was not encrypted.

19. According to the "Notice of Data Event" and "Press Release," Defendant "changed system credentials and took steps to secure its systems and assess relevant company systems that may have been impacted by the event," and is "working with external digital forensic specialists to enhance existing security processes and protocols."

20. According to the "Notice of Data Breach," Defendant "reset passwords for all Artech users, further strengthened [its] existing technical controls, and implemented additional security measures," and "reviewed [its] policies and procedures relating to data security and [is] conducting additional employee training."

21. Defendant's "Notice of Data Breach" acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by advising recipients of the notice – such as Plaintiffs and Class Members – to "remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity."

22. Defendant's "Notice of Data Breach" advises victims to consider "plac[ing] a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing

information in your credit report without express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent."

23. Defendant's "Data Breach Notices" also advise victims to report incidents of fraud and identity theft to the Federal Trade Commission, local law enforcement, and/or their state's attorney general.

24. Although it appears Defendant knew of the Data Breach no later than January 8, 2020, Defendant took no steps to directly notify Plaintiffs or Class Members until September 4, 2020, when Defendant began mailing "Notice of Data Breach" letters. This was a delay of not less than 240 days.

25. The Data Breach resulted in the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, use and/or viewing of unsecured PII of Plaintiffs and Class Members.

26. As a result of the Data Breach, the security and privacy of Plaintiffs' and Class Members' PII was compromised.

The California Attorney General Notice

27. On or about September 4, 2020, Defendant filed with California's Attorney General a sample "Notice of Data Breach" letter (attached hereto as **Exhibit 2**), a "Notice of Data Event" statement (attached hereto as **Exhibit 3**), and a "Press Release" (attached hereto as **Exhibit 4**) that mirrored the language of letters Defendant sent to Plaintiffs and Class Members.

28. The sample "Notice of Data Breach" letter, "Notice of Data Event" statement, and "Press Release" were each filed with California's Attorney General in accordance with California Civ. Code § 1798.82(f).

29. Pursuant to California Civ. Code § 1798.82(f), "[a] person or business that is required to issue a security breach notification pursuant to [§ 1798.82(a)] to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General."

30. Plaintiffs' and Class Members' PII is "personal information" as defined by California Civ. Code § 1798.82(h).

31. Pursuant to California Civ. Code § 1798.82(a), data breach notification letters are sent to residents of California "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system."

32. California Civ. Code § 1798.82(g) defines "breach of the security of the system" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."

33. The Data Breach was a "breach of the security of the system" as defined by California Civ. Code § 1798.82(g).

34. Thus, Defendant filed with California's Attorney General and disseminated these breach notifications because Plaintiffs' and Class Members' unencrypted PII was acquired by an unauthorized person or persons as a result of the Data Breach.

35. Defendant reasonably believes Plaintiffs' and Class Members' unencrypted PII was acquired by an unauthorized person as a result of the Data Breach.

36. The security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted PII was compromised by Defendant as a result of the Data Breach.

37. Defendant reasonably believes the security, confidentiality, or integrity of Plaintiffs' and Class Members' unencrypted PII was compromised by Defendant as a result of the Data Breach.

38. Defendant reasonably believes Plaintiffs' and Class Members' unencrypted PII that was acquired by an unauthorized person as a result of the Data Breach was viewed by unauthorized persons.

39. It is reasonable to infer that Plaintiffs' and Class Members' unencrypted PII that was acquired by an unauthorized person as a result of the Data Breach was viewed by unauthorized persons.

40. It should be rebuttably presumed that Plaintiffs' and Class Members' unencrypted PII that was acquired by an unauthorized person as a result of the Data Breach was viewed by unauthorized persons.

41. After receiving letters sent pursuant to California Civ. Code § 1798.82(a) – and filed with the Attorney General of California in accordance with California Civ. Code § 1798.82(f) – it is

reasonable for recipients, including Plaintiffs and Class Members in this case, to believe that the risk of future harm (including identity theft) is substantial, real and imminent, and to take steps to mitigate that substantial risk of future harm.

Defendant Expressly Promised to Protect Plaintiffs' and Class Members' PII

42. Defendant's Privacy Policy[1] states, as relevant: "Artech respects and is committed to protecting your privacy." … "At no time [] will Artech, sell, trade, rent or distribute personal information to any outside organization."

43. Notwithstanding the foregoing promises, Defendant failed to protect the PII of Plaintiffs and Class Members, as conceded in Defendant's Data Breach Notices.

44. If Defendant truly understood the importance of safeguarding Plaintiffs' and Class Members' PII, it would acknowledge its responsibility for the harm it has caused, and would compensate Plaintiffs and Class Members, provide long-term protection for Plaintiffs and Class Members, agree to Court-ordered and enforceable changes to its cybersecurity policies and procedures, and adopt regular and intensive training to ensure that a data breach like this never happens again.

45. Defendant's data security obligations were particularly important given the known substantial increase in data breaches in various industries, including the recent massive data breaches involving Yahoo, First American Financial Corp., Facebook, Equifax, Marriott, Anthem, Twitter, Target, Home Depot, LabCorp, Quest Diagnostics, and many others. And, given the wide publicity given to these data breaches, there is no excuse for Defendant's failure to adequately protect Plaintiffs' and Class Members' PII.

46. Plaintiffs' and Class Members' PII is now in the hands of cyber criminals who have and will continue to use it for their gain and to the detriment of Plaintiffs and Class Members. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to Plaintiffs and Class Members.

//

[1] *Privacy Policy*, https://www.artech.com/privacy-policy/ (last visited Oct. 27, 2020).

Defendant had an Obligation to Protect Plaintiffs' and Class Members' PII

47. Defendant had obligations created by California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), California's Consumer Privacy Act (Cal. Civ. Code § 1798.100 *et seq.*), common law, and based on industry standards, to keep the compromised PII confidential and to protect it from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, use and/or viewing. Plaintiffs and Class Members provided their PII to Defendant with the common sense understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, use and/or viewing.

48. Defendant's data security obligations and promises were particularly important given the substantial increase in data breaches, which were widely known to the public and to anyone in Defendant's industry.

49. Defendant failed to spend sufficient resources on data security and training its employees to identify data security threats and weaknesses and defend against them.

50. Defendant's security failures demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data leaks, data breaches, and cyber-attacks; and

b. Adequately protecting Plaintiffs' and Class Members' PII.

51. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

52. Defendant is also required (by the CCRA, the CCPA, and various other states' laws and regulations) to protect Plaintiffs' and Class Members' PII, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

//

53. In addition to its obligations under federal and state statutes, Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being accessed by, acquired by, appropriated by, compromised by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, misused by, and/or viewed by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and Class Members.

54. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to design, maintain, and test its computer systems to ensure that the PII in Defendant's possession was adequately secured and protected.

55. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

56. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

57. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

58. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to adequately train and supervise its employees to identify data security threats and weaknesses and defend against them.

59. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to adequately train and supervise its employees to detect a breach on its data security systems in a timely manner.

//

//

60. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from unauthorized access, acquisition, appropriation, compromise, disclosure, encumbrance, exfiltration, release, theft, use and/or viewing because such an inadequacy would be a material fact in the decision to entrust PII with Defendant.

61. Defendant owed a duty to Plaintiffs and Class Members whose PII was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

62. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

It is Well Established That Data Breaches Lead to Identity Theft and Other Harms

63. Plaintiffs and Class Members have been injured by the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use and/or viewing of their PII as a result of the Data Breach.

64. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[2] With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: opening new financial accounts in the victim's name, taking out loans in the victim's name, obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[3]

//

[2] *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited Apr. 30, 2020).

[3] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Apr. 30, 2020).

65. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell and trade the information on the cyber black-market for years.

66. This is not just speculative. As the FTC has reported, if hackers get access to PII, they ***will*** use it.[4]

67. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[5] Identity thieves can also use the information stolen from Plaintiffs and Class Members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

68. Medical identity theft is one of the forms of identity theft that is most common, most expensive, and most difficult to prevent. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[6]

69. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[7]

70. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social

---

[4] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Apr. 30, 2020).

[5] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Apr. 30, 2020).

[6] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited Apr. 30, 2020).

[7] *Id.*

Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI can go from $20 say up to – we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[8] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[9]

71. If, moreover, cyber criminals also manage to acquire financial information, credit and debit cards, health insurance information, driver's licenses and passports, there is no limit to the amount of fraud to which Defendant has exposed Plaintiffs and Class Members.

72. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[10] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

73. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[11]

74. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

//

---

[8] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Apr. 30, 2020).

[9] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Apr. 30, 2020).

[10] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 30, 2020).

[11] *Id.* at 2, 9.

75. There may be a time lag between when sensitive PII is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

76. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, and other PII directly on various Internet websites making the information publicly available.

77. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

78. Medical computer systems are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[14] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

//

//

[12] *Id*. at 29 (emphasis added).

[13] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Apr. 30, 2020).

[14] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited Apr. 30, 2020).

79. Furthermore, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[15]

80. To date, other than providing 12-24 months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do the following:

- remain vigilant against incidents of identity theft and fraud;
- review account statements;
- monitor credit reports for suspicious activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs' and Class Members' PII.

81. Defendant's failure to adequately protect Plaintiffs' and Class Members' PII has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

82. Defendant's offer of 12-24 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft

[15] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Apr. 30, 2020).

monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[16] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

83. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, substantial and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

84. Plaintiffs and Class Members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

[16] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited Apr. 30, 2020).

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' PII, for which there is a well-established and quantifiable national and international market;

i. Damage to their credit due to fraudulent use of their PII; and

j. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

85. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

86. Defendant itself acknowledged the harm caused by the Data Breach by offering Plaintiffs and Class Members 12-24 months of identity theft monitoring services. 12-24 months of identity theft monitoring is woefully inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiffs and Class Members for the injuries they have already suffered.

PUBLIC BENEFIT

87. The causes of action herein are not brought solely on behalf of Plaintiffs and Class Members, but are also brought on behalf of the general public and are intended to benefit the general public to the greatest extent permitted – this includes, but is not necessarily limited to, injunctive relief, with the primary purpose of such injunctive relief being to enjoin Defendant's acts and/or omissions that threaten future injury to the general public.

CLASS ALLEGATIONS

88. Plaintiffs bring this class action lawsuit individually and on behalf of the following proposed Nationwide Class, California Sub-Class, and North Carolina Sub-Class under Rule 23 of the Federal Rules of Civil Procedure.

Nationwide Class: All persons in the United States whose PII was compromised as a result of the Artech Data Breach announced by Artech on or around September 4, 2020.

California Sub-Class: All persons in California whose PII was compromised as a result of the Artech Data Breach announced by Artech on or around September 4, 2020.

North Carolina Sub-Class: All persons in North Carolina whose PII was compromised as a result of the Artech Data Breach announced by Artech on or around September 4, 2020.

89. Plaintiffs reserve the right to modify, change, or expand the definition of the Nationwide Class, California Sub-Class, and North Carolina Sub-Class, or to propose alternative or additional sub-classes based on discovery and further investigation.

90. The Nationwide Class, California Sub-Class, and North Carolina Sub-Class are collectively referred to throughout this Complaint as the "Class," unless otherwise specified.

91. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the designated protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

92. **Numerosity:** Plaintiffs do not know the exact number of Class Members, but believe the Class comprises tens of thousands of individuals throughout the United States. As such, Class Members are so numerous that joinder of all members is impracticable.

93. **Commonality:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' PII;

c. Whether Defendant failed to protect Plaintiffs' and Class Members' PII properly and/or as promised;

d. Whether Defendant's computer system and data security practices used to protect Plaintiffs' and the Class Members' PII violated statutory law, common law, or Defendant's duties;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII;

f. Whether Defendant violated the consumer protection statutes, data breach notification statutes, and/or state privacy statutes applicable to Plaintiffs and Class Members;

g. Whether Defendant failed to notify Plaintiffs and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

h. Whether Defendant acted negligently in failing to safeguard Plaintiffs' and Class Members' PII;

i. Whether Defendant breached implied contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII, and to have reasonable data security measures;

j. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

l. What equitable relief is appropriate to redress Defendant's wrongful conduct; and

m. What injunctive relief is appropriate to redress the imminent and currently ongoing harm and risk of future harm faced by Plaintiffs and Class Members.

94. **Typicality:** Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs and Class Members were injured through Defendant's uniform misconduct and their legal claims arise from the same core practices of Defendant.

95. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members and has retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class Members, and there are no defenses unique to Plaintiffs. Plaintiffs and Plaintiffs' counsel are committed to prosecuting this action

vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiffs nor Plaintiffs' counsel have any interest adverse to those of the other Class Members.

96. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23 because prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendant's computer system still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of Defendant's computer system.

97. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

98. **Predominance:** The proposed action meets the requirements of Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the Class predominate over any questions that may affect only individual Class Members in the proposed Class.

99. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ. P. 23(b)(3) because a class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant. Even if it were economically feasible, requiring tens of thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

100. **Certification of Particular Issues:** In the alternative, this action may be maintained as a class action with respect to particular issues in accordance with Fed. R. Civ. P. 23(c)(4).

101. Finally, all members of the proposed Nationwide Class and California Sub-Class are readily ascertainable. Defendant has access to addresses and other contact information for members of the Class, which can be used to identify Class Members.

COUNT I

NEGLIGENCE

102. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

103. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

104. Defendant collected and stored the PII of Plaintiffs and Class Members.

105. Plaintiffs and Class Members were required by Defendant to provide their PII to Defendant as a condition of their registration with Defendant.

106. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII of Plaintiffs and Class Members.

107. Defendant owed duties of care to Plaintiffs and Class Members whose PII had been entrusted with Defendant.

108. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

109. Defendant acted with wanton disregard for the security of Plaintiffs' and Class Members' PII. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII in computer systems, such as theirs.

110. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with Plaintiffs and Class Members by placing their PII in Defendant's computer system – information that Plaintiffs and Class Members had been required to provide to Defendant.

//

//

111. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

112. Pursuant to California's Customer Record's Act (Cal. Civ. Code § 1798.80, *et seq.*), Defendant had a duty to disclose any breach of Plaintiff Poling's and Class Members' PII in the most expedient time possible and without unreasonable delay.

113. Pursuant to California's Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff Poling's and Class Members' PII.

114. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

115. Defendant breached its duties to Plaintiff Poling and Class Members under California's Customer Record's Act (Cal. Civ. Code § 1798.80, *et seq.*) by failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay.

116. Defendant breached its duties to Plaintiff Poling and Class Members under California's Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Class Members' PII.

117. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

118. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, including those duties under the Federal Trade Commission Act, California's Customer Record's Act, and California's Consumer Privacy Act, Plaintiffs and Class Members would not have been injured.

119. The injury and harm that has occurred is the type of harm the Federal Trade Commission Act, California's Customer Record's Act, and California's Consumer Privacy Act were intended to guard against.

//

120. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class Members to suffer the foreseeable harms associated with the exposure of their PII.

121. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and continue to face an increased risk of suffering future injury and, as such, are entitled to damages in an amount to be proven at trial.

COUNT II

INVASION OF PRIVACY

122. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

123. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

124. California established the right to privacy in Article 1, Section 1 of the California Constitution.

125. Both the State of California and the State of North Carolina recognize the tort of Intrusion into Private Affairs, and adopt the formulation of that tort found in the Restatement (Second) of Torts which states:

126. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts § 652B (1977).

127. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to and acquisition by unauthorized third parties.

128. Defendant owed a duty to its registrants, including Plaintiffs and Class Members, to keep their PII confidential.

//

//

129. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the type of information that is the subject of this action, is highly offensive to a reasonable person.

130. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of their use of Defendant's services, but privately, with the intention that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

131. The Data Breach constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

132. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

133. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

134. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

135. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

136. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

//

//

COUNT III

UNJUST ENRICHMENT

137. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

138. This count is brought on behalf of all the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

139. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they utilized Defendant's services and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and have their PII protected with adequate data security.

140. Defendant knew that Plaintiffs and Class Members conferred a benefit that Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

141. The amounts that Defendant profited from Plaintiffs' and Class Members' use of its services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

142. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by statutory and common law as well as industry standards.

143. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

144. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

145. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to use Defendant's services.

146. Plaintiffs and Class Members have no adequate remedy at law.

147. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of

the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

148. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including a substantial and imminent risk of identity theft.

149. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them or that it unjustly received by doing business with them. In the alternative, Defendant should be compelled to refund to Plaintiffs and Class Members the amounts that Plaintiffs and Class Members or others overpaid for Defendant's services.

COUNT IV

BREACH OF FIDUCIARY DUTY

150. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

151. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

152. In light of their special relationship, Defendant has become the guardian of Plaintiffs' and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its registrants' PII, to act primarily for the benefit of its registrants, including Plaintiffs and Class

Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

153. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

154. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

155. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

BREACH OF CONFIDENCE

156. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

157. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Class.

158. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PII that Plaintiffs and Class Members provided to Defendant.

159. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

160. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by any unauthorized third parties.

161. Plaintiffs and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

162. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

163. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

164. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

165. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' PII, as well as the resulting damages.

166. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs' and Class Members' PII had security and other vulnerabilities that placed Plaintiffs' and Class Members' PII in jeopardy.

167. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Defendant's services they received.

168. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

//

COUNT VI

BREACH OF IMPLIED CONTRACT

169. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

170. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

171. When Plaintiffs and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect their PII and to timely notify them in the event of a data breach.

172. Defendant required its registrants (including Plaintiffs and Class Members) to provide PII in order to register with Defendant.

173. Based on the implicit understanding, Plaintiffs and Class Members accepted Defendant's offers and provided Defendant with their PII.

174. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII as promised or provide timely notice of a data breach.

175. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

176. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach.

177. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of the implied contract with Plaintiffs and Class Members.

COUNT VII

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

178. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

179. This count is brought on behalf of the Nationwide Class or, alternatively, the California and North Carolina Sub-Classes.

//

180. As described above, when Plaintiffs and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect their PII and to timely notify them in the event of a data breach.

181. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

182. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations (including California's UCL), and when it engaged in unlawful practices under other laws. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII; and failing to disclose to Plaintiffs and Class Members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

183. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

184. Likewise, all conditions required for Defendant's performance were met.

185. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

186. Plaintiffs and Class Members have been harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

187. Defendant is liable for this breach of these implied covenants whether or not it is found to have breached any specific express contractual term.

188. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

//

COUNT VIII

VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code §17200, *et seq.*

189. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

190. This count is brought on behalf of the Nationwide Class or, alternatively, the California Sub-Class.

191. Defendant does business in California and with California residents. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and/or promising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class Members' PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing; representing and/or promising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' PII; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII;

b. by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment;

c. by violating California's Customer Records Act (Cal. Civ. Code §1798.80, *et seq.*);

d. by violating the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 *et seq.*); and

e. by violating the Federal Trade Commission Act (15 U.S.C. §45).

192. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect personal data and

ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, and the CCRA, Cal. Civ. Code § 1798.81.5.

193. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

194. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

195. Plaintiffs seek relief under the UCL, including restitution to Class Members of money or property that Plaintiffs and Class Members lost, or that Defendant may have acquired, by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

COUNT IX

VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code § 1798.80, *et seq.*

196. Plaintiffs incorporates the foregoing allegations as if fully set forth herein.

197. This count is brought on behalf of the California Sub-Class.

198. Section 1798.82 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

//

199. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

200. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

201. The Data Breach described herein constituted a "breach of the security system" of Defendant.

202. As alleged above, Defendant unreasonably delayed (not less than 240 days) informing Plaintiffs and Class Members about the Data Breach, affecting their PII, after Defendant knew the Data Breach had occurred.

203. Defendant failed to disclose to Plaintiffs and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when Defendant knew or reasonably believed such information had been compromised.

204. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

205. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiffs and the Class Members would impede its investigation.

206. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class Members because their stolen information would have had less value to identity thieves.

207. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

208. Plaintiffs and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiffs and the other Class Members as alleged above and equitable relief.

209. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiffs and Class Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under

Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiffs and Class Members and despicable conduct that has subjected Plaintiffs and Class Members to hardship in conscious disregard of their rights. As a result, Plaintiffs and Class Members are entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

COUNT X

VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT

Cal. Civ. Code § 1798.100, *et seq.*

210. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

211. This count is brought on behalf of the California Sub-Class.

212. Through the above-detailed conduct, Defendant violated California's Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100, et seq.) by subjecting the nonencrypted and nonredacted PII of Plaintiffs and Class Members to unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

213. In accordance with Cal. Civ. Code § 1798.150(b), prior to the filing of this Complaint, Plaintiffs' counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

214. On behalf of Class Members, Plaintiffs seek injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to respond to Plaintiffs' notice letter or agree to rectify the violations detailed above, Plaintiffs will also seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

COUNT XI

INJUNCTIVE / DECLARATORY RELIEF

215. Plaintiffs incorporates the foregoing allegations as if fully set forth herein.

//

216. This count is brought on behalf of all the Nationwide Class or, alternatively, the California Sub-Class.

217. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

218. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiffs and Class Members.

219. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII.

220. Defendant still possess PII regarding Plaintiffs and Class Members.

221. Since the Data Breach, Defendant has announced few if any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

222. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

223. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

224. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

225. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests,

and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective registrants about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request the Court order relief and enter judgment in their favor and against Artech as follows:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein.

//

B. Plaintiffs request injunctive and other equitable relief as is necessary to protect the interests of the Class, including (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with the CCRA, other federal, state and local laws, and best practices under industry standards; (iii) requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected; (iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner; (v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering it to promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendant to implement multi-factor authentication requirements; (viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; (ix) requiring Defendant to encrypt all PII; (x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (xi) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; (xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII no longer necessary for the provision of services; (xiii) requiring Defendant to conduct regular computer system scanning and security checks; (xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members; and (xvi) requiring Defendant to educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as steps Class Members must take to protect themselves.

//

//

C. A judgment awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendant pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

DATED: July 16, 2021

GREEN & NOBLIN, P.C.

By: /s/ Robert S. Green
Robert S. Green

James Robert Noblin
Evan M. Sumer
2200 Larkspur Landing Circle, Suite 101
Larkspur, CA 94939
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
Email: gnecf@classcounsel.com

Cornelius P. Dukelow*
cdukelow@abingtonlaw.com
Oklahoma Bar No. 19086
ABINGTON COLE + ELLERY
320 South Boston Avenue
Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)

William B. Federman*
wbf@federmanlaw.com
Oklahoma Bar No. 2853
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112

**Admitted Pro Hac Vice*

Counsel for Plaintiff and the Proposed Class